NSE7_SAC-6.2^{Q&As}

Fortinet NSE 7 - Secure Access 6.2

Pass Fortinet NSE7_SAC-6.2 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/nse7_sac-6-2.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

Which two EAP methods can use MSCHAPV2 for client authentication? (Choose two.)

A. PEAP

B. EAP-TTLS

C. EAP-TLS

D. EAP-GTC

Correct Answer: AC

Reference: https://help.fortinet.com/fauth/3-3/Content/FortiAuthenticator%203_3%20Admin%
20Guide/500/501_EAP.htm

QUESTION 2

Default VLANs are created on FortiGate when the FortiLink interface is created. By default, which VLAN is set as
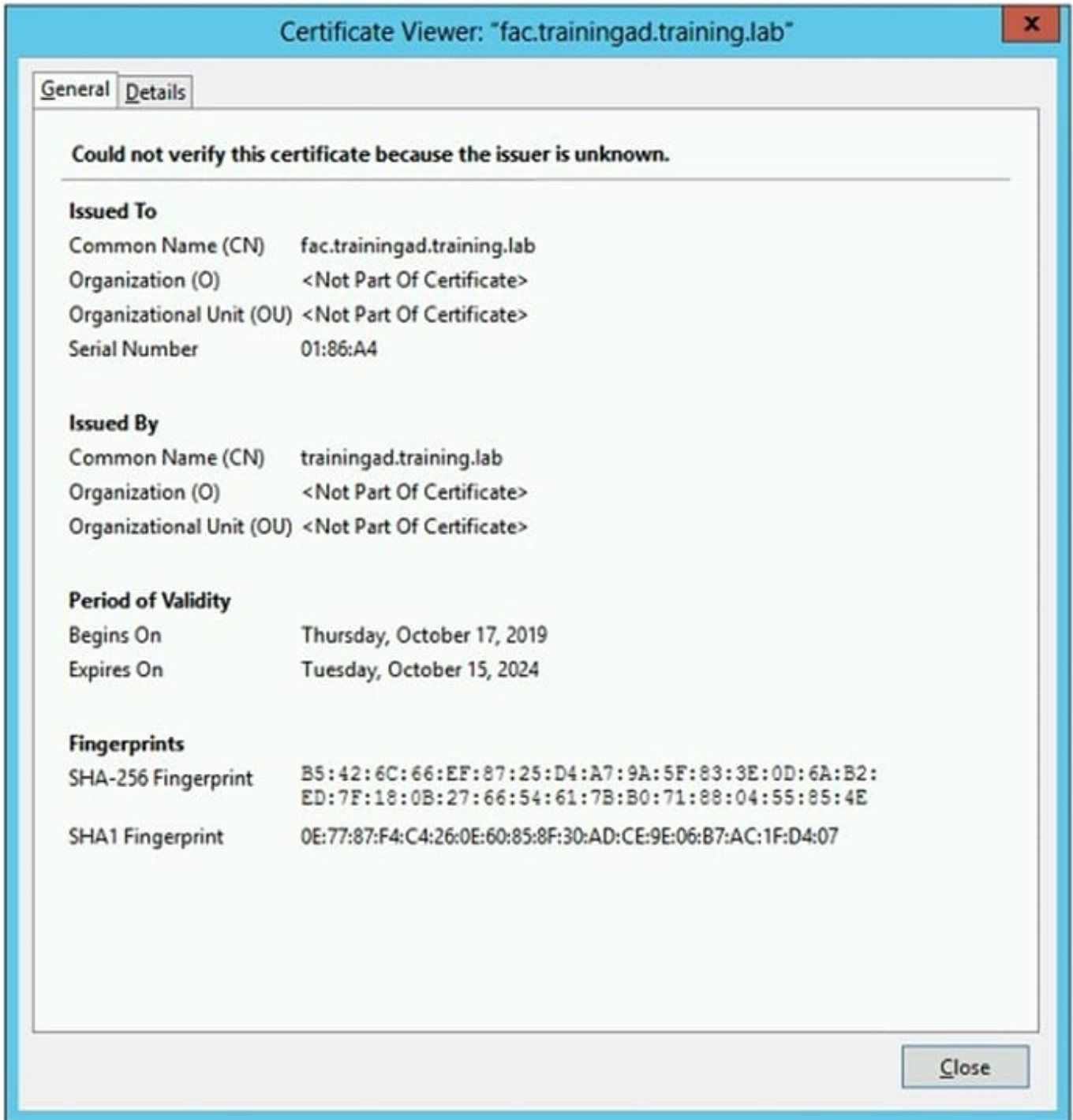Allowed VLANs on all FortiSwitch ports?

A. Sniffer VLAN

B. Camera VLAN

C. Quarantine VLAN

D. Voice VLAN

Correct Answer: A

QUESTION 3

Refer to the exhibit showing certificate values.

![Pass2Lead](https://Pass2Lead.com)
Certificate Viewer: "fac.trainingad.training.lab"

General | Details

Could not verify this certificate because the issuer is unknown.

Issued To

Common Name (CN)	fac.trainingad.training.lab
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	<Not Part Of Certificate>
Serial Number	01:86:A4

Issued By

Common Name (CN)	trainingad.training.lab
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	<Not Part Of Certificate>

Period of Validity

Begins On	Thursday, October 17, 2019
Expires On	Tuesday, October 15, 2024

Fingerprints

SHA-256 Fingerprint	B5:42:6C:66:EF:87:25:D4:A7:9A:5F:83:3E:0D:6A:B2:ED:7F:18:0B:27:66:54:61:7B:B0:71:88:04:55:85:4E
SHA1 Fingerprint	0E:77:87:F4:C4:26:0E:60:85:8F:30:AD:CE:9E:06:B7:AC:1F:D4:07

Close

Wireless guest users are unable to authenticate because they are getting a certificate error while loading the captive portal login page. This URL string is the HTTPS POST URL guest wireless users see when attempting to access the network using the web browser:

https://fac.trainingad.training.com/guests/login/?loginandpost=https://auth.trainingad.training.1ab:1003/fgtauthandmagic =000a038293d1f411andusermac=b8:27:eb:d8:50:02andapmac=70:4c:a5:9d:0d:28andapip=10.10.100.2anduserip=10.0 .3.1andssid=Guest03andapname=PS221ETF18000148andbssid=70:4c:a5:9d:0d:30

Which two settings are the likely causes of the issue? (Choose two.)

A. The external server FQDN is incorrect.

![Pass2Lead](https://Pass2Lead.com)
B. The FortiGate authentication interface address is using HTTPS.

C. The wireless user\\'s browser is missing a CA certificate.

D. The user address is not in DDNS form.

Correct Answer: AC

QUESTION 4

Which step can be taken to ensure that only FortiAP devices receive IP addresses from a DHCP server on FortiGate?

A. Change the interface addressing mode to FortiAP devices.

B. Create a reservation list in the DHCP server settings.

C. Configure a VCI string value of FortiAP in the DHCP server settings.

D. Use DHCP option 138 to assign IPs to FortiAP devices.

Correct Answer: C

QUESTION 5

802.1X port authentication is enabled on only those ports that the FortiSwitch security policy is assigned to.

Which configurable items are available when you configure the security policy on FortiSwitch? (Choose two.)

A. FSSO groups

B. Security mode

C. User groups

D. Default guest group

Correct Answer: BC

[Latest NSE7_SAC-6.2 Dumps](#)   [NSE7_SAC-6.2 PDF Dumps](#)   [NSE7_SAC-6.2 Practice Test](#)